REMARKS

The Office Action dated July 13, 2009, has been received and carefully considered. In this response, claim 1 has been amended. No new matter has been added. Entry of the amendments to claim 1 is respectfully requested. Reconsideration of the current rejections in the present application is also respectfully requested based on the following remarks.[1]

I. THE § 1.131 AFFIDAVIT SHOULD BE ACCEPTED

Applicant filed an Affidavit under 37 C.F.R. § 1.131 with the March 26, 2009 Response. The Affidavit showed conception before the filing date of the Blake reference, cited below. In response, the Examiner asserts that the Affidavit is "ineffective to overcome the Blake reference." Office Action, page 2. The Examiner noted that "Applicant has submitted a declaration asserting diligence, but many of the statements are ambiguous such as "meetings" and "emails discussing development." These statements are insufficient to show due

[1] As Applicant's remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicant's silence as to assertions made by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., assertions regarding dependent claims, whether a reference constitutes prior art, whether references are legally combinable for obviousness purposes) is not a concession by Applicant that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute such in the future.

diligence." Office Action, page 2.

Applicant respectfully disagrees. Applicant notes that the declaration includes as an attachment a detailed functional requirements document. Applicant also notes that paragraph 5 of the declaration outlines with detail, including recipients and dates, communications regarding the subject matter of the application. Based on this detailed description, Applicants respectfully submit that the declaration should be accepted, and that the Blake reference should be withdrawn.

In further support of the filed declaration, Applicant respectfully submits copies of the documents listed in paragraph 5, subsections a-i. The documents are submitted as exhibits to this Response, and the Exhibit letter matches the subsection of paragraph 5 (i.e., Exhibit A includes the materials referenced in paragraph 5, subsection a, etc.) Applicant respectfully submits that the attachments show sufficient evidence of conception, diligence, and reduction to practice, and so the declaration submitted under 37 C.F.R. § 1.131 should be accepted.

II. THE OBVIOUSNESS REJECTION OF CLAIMS 1-4, 7, 8, 13-15, 17-20, AND 21-24

On pages 3-5 of the Office Action, claims 1-4, 7, 15, 18-20, 23, and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0128543 to Blake ("Blake") in view of U.S. Patent Application Publication No. 2004/0139128 to Becker ("Becker"). This rejection is hereby respectfully traversed.

On page 5 of the Office Action, claim 6 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Blake in view of U.S. Patent Application Publication No. 2004/0078592 to Fagone ("Fagone"). This rejection is hereby respectfully traversed. Applicant notes that claim 6 was respectfully canceled without prejudice in a Response dated November 14, 2008, and so Applicant respectfully requests that this rejection be withdrawn.

On pages 5-6 of the Office Action, claim 8 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Blake in view of Becker in view of Schlereth "Analysis of a Compromised Honeypot on a Cable Modem" ("Schlereth"). This rejection is hereby respectfully traversed.

On pages 6-7 of the Office Action, claims 13 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over

Blake in view of Becker in view of U.S. Patent Application Publication No. 2003/0110396 to Lewis ("Lewis"). This rejection is hereby respectfully traversed.

On page 7 of the Office Action, claim 17 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Blake in view of Becker in view of INFOCUS: The Honeynet Project ("INFOCUS"). This rejection is hereby respectfully traversed.

On pages 7-8 of the Office Action, claims 21 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Blake in view of Becker in view of U.S. Patent Application Publication No. 2005/01084156 to Turk ("Turk"). This rejection is hereby respectfully traversed.

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074 (Fed. Cir. 1988). There are four separate factual inquiries to consider in making an obviousness determination: (1) the scope and content of the prior art; (2) the level of ordinary skill in the field of the invention; (3) the differences between the claimed invention and the prior art; and (4) the existence of any objective evidence, or "secondary considerations," of non-obviousness. Graham v. John Deere Co., 383 U.S. 1, 17-18 (1966); see also KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007). An "expansive and flexible

approach" should be applied when determining obviousness based on a combination of prior art references. KSR, 127 S. Ct. at 1739. However, a claimed invention combining multiple known elements is not rendered obvious simply because each element was known independently in the prior art. Id. at 1741. Rather, there must still be some "reason that would have prompted" a person of ordinary skill in the art to combine the elements in the specific way that he or she did. Id.; In re Icon Health & Fitness, Inc., 496 F.3d 1374, 1380 (Fed. Cir. 2007). Also, modification of a prior art reference may be obvious only if there exists a reason that would have prompted a person of ordinary skill to make the change. KSR, 127 S. Ct. at 1740-41.

Applicants respectfully submit that the Blake reference should be withdrawn for at least the reasons stated above in view of the 37 C.F.R. § 1.131 declaration and supporting documents. Assuming, *arguendo*, that the Blake reference is prior art, the combination of Blake and Becker is still not appropriate.

The Examiner notes that "[i]t would have been obvious to one of ordinary skill in the art to use the image of Becker with the redeployment of Blake because it would restore the honeypot after a compromise." Office Action, page 4. Applicant respectfully notes that the honeypot in Blake is specifically

designed to "morph." See Blake, Abstract. The honeypot is not redeployed "by reinitializing the state of the honey pot to an initial state in which the honey pot was in at the time it was deployed," as recited in claim 1. The honeypot in Blake is expected to morph in order to "change its characteristics to entice a malicious user to something that the malicious user might consider as more vulnerable, exploitable, and, therefore, more interesting." Blake, paragraph [0084]. Paragraph [0036] and Figure 3 disclose a "typical" honeypot, and disclose four modes of operation: a configuration phase, where the honeypot is configured; an emulation phase, where the honeypot is operated while information about requests is logged; an analysis phase, where the logged information is studied; and a reconfiguration phase, where "an administrative user determines whether the configuration of the honeypot should be changed." None of these steps, however, discloses at least steps to "automatically redeploy the honey pot, including by reinitializing the state of the honey pot to an initial state in which the honey pot was in at the time it was deployed. . .," as recited in claim 1.

It would therefore not have been appropriate to modify the disclosure of Blake with the Becker reference, as the Blake reference discloses a morphing honeypot, and the Becker reference is directed to "a system and method of backing up a

computer system." Becker, Title. There is no need to redeploy a morphing honeypot, as the morphing honeypot is reconfigured. *See* Blake, Figure 6, element 616.

In view of the foregoing, Applicant respectfully submits that claim 1 should be allowable over Blake and Becker.

Regarding claims 2-4, 7, 15, and 18-20, these claims are dependent upon independent claim 1. If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071 (Fed. Cir. 1988). Thus, since independent claim 1 should be allowable as discussed above, claims 2-4, 7, 15, and 18-20 should also be allowable at least by virtue of their dependency on independent claim 1. Moreover, these claims recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination. For example, claim 19 recites a method "further including saving state information associated with the honey pot and wherein saving and redeploying occur in parallel."

Applicant respectfully submits that the aforementioned obviousness rejection of claims 6, 8, 13, 14, 17, 21, and 22 has become moot in view of the deficiencies of the primary references (i.e., Blake and Becker) as discussed above with respect to independent claim 1. That is, claims 6, 8, 13, 14,

17, 21, and 22 are dependent upon independent claim 1 and thus inherently incorporate all of the limitations of independent claim 1. Also, the secondary references (i.e., Fagone, Schlereth, Lewis, INFOCUS, and Turk) fail to disclose, or even suggest, the deficiencies of the primary references as discussed above with respect to independent claim 1. Indeed, the Examiner does not even assert such. Thus, the combination of the secondary references with the primary references also fails to disclose, or even suggest, the deficiencies of the primary references as discussed above with respect to independent claim 1. Accordingly, claims 6, 8, 13, 14, 17, 21, and 22 should be allowable over the combination of the secondary reference with the primary references at least by virtue of their dependency on independent claim 1. Moreover, claims 6, 8, 13, 14, 17, 21, and 22 recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

Regarding claims 23 and 24, these claims, while of different scope than claim 1, recite subject matter related to claim 1. Thus, the arguments set forth above with respect to claim 1 are equally applicable to claims 23 and 24. Accordingly, Applicant respectfully submits that claims 23 and

24 should be allowable over Blake and Becker for the same reasons as set forth above with respect to claim 1.

In view of the foregoing, Applicant respectfully requests that the aforementioned obviousness rejection of claims 1-4, 7, 8, 13-15, 17-20, and 21-24 be withdrawn.

III. CONCLUSION

In view of the foregoing, Applicant respectfully submits that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

Respectfully submitted,

Hunton & Williams LLP

By: _____
Thomas E. Anderson
Registration No. 37,063

TEA:JBB

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Date: October 13, 2009

Exhibit A

Goal

The goal for the honey pot system is to semi-automatically capture malicious code samples and detect new attacks.

Broad Requirements

The diverse nature of the targets of attack (at the operating system and application level) requires that the system be capable of supporting multiple honey pots and multiple operating systems, thus permitting the broadest coverage possible.

The large amount of "background noise" (known malicious code and attacks that are continually launched across the Internet) requires that the system be capable of recognizing known attacks and known malicious code, thus permitting analysts to focus on those incidents that are more likely to result in the capture of unknown malicious code or novel attacks.

The high frequency of known attacks and known malicious code requires that the system be capable of automatically detecting an incident, capturing relevant data, and reinitializing the honey pot to capture the next incident, thus freeing analysts from this repetitive task that may occur at any time of day.

Virtual Honey Pot

Given these requirements and after performing some research I recommend a virtual honey pot approach. Virtual honey pots execute as a process within a normal host.

A virtual honey pot approach will permit us to run multiple honey pots in a single host, making deployment and management easier, and permitting us to somewhat fulfill the first requirement.

It is not uncommon for the host the executing the virtual honey pot to have access to the virtual honey pot's environment (e.g. its file system), thus making automated analysis easier, thus permitting us to somewhat fulfill the second requirement.

In addition, some virtualization systems support API's to control the environment, for instances to start-up or shutdown a virtual host, thus permitting us to fulfill the third requirement.

Furthermore, some virtualization systems store their state in regular file, which makes management and automation of the system easier, and permit us to easily archive incidents for latter analysis.

VMware

The only real competitor in the area of virtual operating environments is VMware. The offer three products: VMware Workstation, VMware GSX Server, and VMware ESX Server.

After reviewing them VMware GSX Server best fits our needs:

- It supports multiple concurrent virtual hosts.
- It supports a broad range of guest operating systems: Windows .NET, Windows 2000/NT, Window Me, Window 9x, WfW, Windows 3.1, MS-DOS, Linux, and FreeBSD. It may also be possible to install other x86-based operating systems such as Solaris, although they are not officially supported.
- It supplies API that permit to programmatically control each virtual host individually.
- Its state, such as the virtual host file system and suspended virtual host memory, are stored in files.
- It supports suspending a virtual host, instead of simply shutting it down.

In addition, the Linux version of VMware GSX Server permits the mounting of the virtual disks as a regular file system (so long as the Linux kernel supports the file system type).

The System

I envision a system running VMware GSX Server with a number of virtual honey pots running different operating systems and applications. The system would automatically detect that a virtual honey pot has been breached by monitoring outgoing network traffic from the virtual honey pot. When the system determines a virtual honey pot has been breached it would suspect the virtual honey pot and copy its state to an analysis area. It would then reinitialize the virtual honey pot so that it can immediately become available for new incidents. After this, the system can aggregate the data collected by or against the virtual honey pot, such as packet dumps and IDS events. It can perform further analysis by mounting the virtual drive and flagging any file changes. It can also scan the virtual drive for known malicious code. Finally, it dumps all the information into a database, which a front-end makes available to analysis for browsing. Analysis can choose to discard an incidents state, archive it, or perform further analysis.

Timeline

I would recommend we build the system in at least two phases.

Phase 1:

This phase emphasizes building the core technology, and collecting and analyzing data in a manner that is independent of the virtual honey pot's operating system or application.

- Build the virtual honey pot hosting environment
  - Setup virtual honey pots.
  - Write monitoring and control scripts.
    - Monitor outgoing virtual honey pot traffic.
- Analysis:
  - Detect file system changes
    - This includes sample collection (new files)
  - Detect known malicious code in the file system
  - Collect network traffic
  - Detect known attacks
    - Run an IDS

Phase 2:

This phase emphasizes augmenting the technology by collecting and analyzing data that is dependent on the virtual honey pot's operating system and/or application.

Platform specific monitoring:

- Syslog / Even Log
- Deleted files
- Registry changes
- API tracing
- Terminal monitoring
  - Keylogger

Exhibit B

Principal: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
$FILE:
AltFrom: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo: StdNotesLtr0
useApplet: True
Sign: 0
DefaultMailSaveOptions: 1
Query_String:
Subject: AQS Product Requirements document
SendTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
CopyTo:
InetSendTo: craig_davison@symantec.com,elias_levy@symantec.com
InetCopyTo:
$StorageTo: 1,1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID: <OFA4511536.833AB0DF-ON87256C77.0081856A-87256C77.0082010A@LocalDomain>
From: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
INetFrom: mario_vanvelzen@symantec.com
PostedDate: 11/20/2002 04:39:59 PM
Encrypt:
RoutingState:
$UpdatedBy: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: A4511536833AB0DF87256C770081856A
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 11/20/2002 04:31:38 PM-11/20/2002 04:31:42 PM
$MsgTrackFlags: 0
DeliveredDate: 11/20/2002 04:31:42 PM

Greetings,

The project is now the Attack Quarantine System (AQS). I have attached the latest Product Requirements document. Changes since the last version:

- added exaustive costing issues
- added plausible attack scenario
- added information regarding maintenance duties of the Threat Analyst Team
- reworded users to include potential SARC and other Response analysts
- minor cosmetic changes (headers, layout)

If you could please review and comment, that would be great.

Cheers,

Mario

Exhibit C

Principal: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
InetSendTo: .
InetCopyTo: dan_hanson@symantec.com
InetBlindCopyTo:
$StorageTo: .
$StorageCc: 1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID: <OF764386C8.9996ADAD-ON87256C85.0009CFB9-87256C85.000A06ED@LocalDomain>
INetFrom: craig_davison@symantec.com
PostedDate: 12/03/2002 06:49:31 PM
Recipients: mvelzen@securityfocus.com,CN=Dan Hanson/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
$UpdatedBy: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
MailOptions: 0
SaveOptions: 1
From: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
AltFrom: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo: stdNotesLtr0
useApplet: True
Sign: 0
Encrypt:
DefaultMailSaveOptions: 1
Query_String:
SendTo: mvelzen@securityfocus.com
CopyTo: CN=Dan Hanson/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
BlindCopyTo:
Subject: 10.0.2.6 (aqs)
EnterSendTo: Mario Van Velzen
EnterCopyTo: CN=Dan Hanson/OU=Calgary/OU=Alberta/O=SYMANTEC
EnterBlindCopyTo:

Do I have an account on that box?

$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID: <OFD7CBF588.29C53A04-ON87256C8E.0063689A-87256C8E.00657EFC@LocalDomain>
INetFrom: craig_davison@symantec.com
PostedDate: 12/13/2002 11:28:36 AM
MailOptions: 0
SaveOptions: 1
$Links:
$AltNameLanguageTags:
$StorageCc: 1,1
$StorageTo: 1
$StorageBcc:
InetCopyTo: elias_levy@symantec.com,mario_vanvelzen@symantec.com
InetSendTo: elias_levy@symantec.com
AltCopyTo:
InetBlindCopyTo:
InheritedReplyTo:
InheritedFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
InheritedAltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
InheritedFromDomain:
From: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
AltFrom: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo: stdNotesLtr0
Sign: 0
Encrypt: 1
DefaultMailSaveOptions: 1

```
Query_String:
Principal:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
SendTo:  CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
CopyTo:  CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@symantec,CN=Mario Van
Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC@symantec
BlindCopyTo:
Subject:  Re: DeepSight AQS
$SealData:
EnterSendTo:  CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
EnterCopyTo:  CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@symantec,CN=Mario Van
Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC@symantec
EnterBlindCopyTo:
$Seal:
$UpdatedBy:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC

$Mailer:  Lotus Notes Release 5.0.9a  January 7, 2002
$MessageID:  <OFA9C1ACA9.7F67D8F7-ON87256C92.0007B301-87256C92.0009BFC7@LocalDomain>
INetFrom:  craig_davison@symantec.com
PostedDate:  12/16/2002 06:46:29 PM
MailOptions:  0
SaveOptions:  1
$AltNameLanguageTags:
$StorageCc:  1,1,1
$StorageTo:  1
$StorageBcc:
InetCopyTo:
InetSendTo:  elias_levy@symantec.com
AltCopyTo:
InetBlindCopyTo:
InheritedReplyTo:
InheritedFrom:  CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
InheritedAltFrom:  CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
InheritedFromDomain:
From:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
AltFrom:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo:  stdNotesLtr0
useApplet:  True
Sign:  0
Encrypt:  1
DefaultMailSaveOptions:  1
Query_String:
Principal:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
SendTo:  CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
CopyTo:
BlindCopyTo:
Subject:  Re: DeepSight AQS
$SealData:
$SealData:
EnterSendTo:  CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC
EnterCopyTo:
EnterBlindCopyTo:
$Seal:
$UpdatedBy:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC

$Mailer:  Lotus Notes Release 5.0.9a  January 7, 2002
$MessageID:  <OF61D81C7A.C4B94B9F-ON87256C8E.0080934B-87256C94.000DDD26@LocalDomain>
INetFrom:  craig_davison@symantec.com
PostedDate:  12/18/2002 07:31:31 PM
Recipients:  mvelzen@securityfocus.com
$UpdatedBy:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
MailOptions:  0
```

```
SaveOptions:  1
$Links:
$AltNameLanguageTags:
$StorageCc:  .
$StorageTo:  1
$StorageBcc:
InetCopyTo:  .
InetSendTo:  elias_levy@symantec.com
AltCopyTo:
InetBlindCopyTo:
InheritedReplyTo:
InheritedFrom:  CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
InheritedAltFrom:  CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
InheritedFromDomain:
From:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
AltFrom:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo:  stdNotesLtr0
Sign:  0
Encrypt:
DefaultMailSaveOptions:  1
Query_String:
Principal:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
SendTo:  CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
CopyTo:  mvelzen@securityfocus.com
BlindCopyTo:
Subject:  Re: DeepSight AQS
$SealData:
EnterSendTo:  CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC
EnterCopyTo:  Mario Van Velzen
EnterBlindCopyTo:
$Seal:

□
$Mailer:  Lotus Notes Release 5.0.9a  January 7, 2002
$MessageID:  <OFA62FCDFF.1822C93B-ON87256C9C.007B16DE-87256C9D.00O4D561@LocalDomain>
INetFrom:  craig_davison@symantec.com
PostedDate:  12/27/2002 05:52:47 PM
Recipients:  CN=Elias Levy/OU=Redwood
City/OU=Cal/O=SYMANTEC@SYMANTEC,mvelzen@securityfocus.com
$UpdatedBy:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
MailOptions:  0
SaveOptions:  1
$Links:
$AltNameLanguageTags:
$StorageCc:  1,.
$StorageTo:  1,.
$StorageBcc:
InetCopyTo:
InetSendTo:  elias_levy@symantec.com,.
AltCopyTo:
InetBlindCopyTo:
InheritedReplyTo:
InheritedFrom:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedAltFrom:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedFromDomain:
From:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
AltFrom:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo:  stdNotesLtr0
Sign:  0
Encrypt:
DefaultMailSaveOptions:  1
Query_String:
Principal:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
```

SendTo: CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC,mvelzen@securityfocus.com
CopyTo:
BlindCopyTo:
Subject: Re: DeepSight AQS
EnterSendTo: CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC,Mario Van Velzen
EnterCopyTo:
EnterBlindCopyTo:

Mario suggested that I combine the fields common to the tables describing incoming data stored as files (File, CapturedPackets, DecryptedTraffic) into a single table, and have separate tables only for type-specific fields like permissions for Files and source/destination addresses for DecryptedTraffic.
The first advantage of this is it would cut down on the number of database queries we'd need to get a unified list of incoming data. As well, new types of data would be easier to integrate with our code.

Also, we could separate the connection information from the DecryptedTraffic table into an IntrusionConnection table. Rows from this table could be joined to CapturedPackets 1:n for multiple protocols/source and destination ports, and joined to DecryptedTraffic 1:1.

We'll call the common table Data:
- ID (unique)
- Data (points to a file, say /var/dionaea/data/<random string>)
- Date/time captured or uploaded
- MD5/other hash
- DataTypes ID

DataTypes:
- ID (unique)
- Type (table names: "File", "CapturedPackets", "DecryptedTraffic" etc.)

Altered File, CapturedPackets, DecryptedTraffic tables:
File:
- ID (unique)
- Original Filename
- Created, Modified, Accessed date/times
- Captured or Uploaded times
- FileTypes ID
- Permissions

CapturedPackets:
- ID (unique)

DecryptedTraffic:
- ID (unique)
- Information about the original SSL traffic
  SSL/TLS version

IntrusionConnection:
- Source IP
- Destination IP
- Source Port for TCP/UDP
- Dest Port for TCP/UDP
- ICMP Type
- Protocol

2002-12-18 07:31 PM

To: Elias Levy/Redwood City/Cal/SYMANTEC
cc: mvelzen@securityfocus.com
Subject: Re: DeepSight AQS

I was talking with Mario a few weeks ago and this idea came up during our discussion:
These tables are by no means comprehensive.

First, a FileTypes table:
- ID (unique)
- Free text ("ELF binary", "Win32 DLL", etc.)

We would store files in a File table:
- ID (unique)
- Original Filename
- Data (points to a file, say /var/dionaea/files/<random string>)
- CRC/hash
- Created, Modified, Accessed date/times
- Captured or Uploaded times
- FileTypes ID
- Permissions

Packet captures in a CapturedPackets table:
- ID (unique)
- Data (points to a file, say /var/dionaea/packetcap/<random string>)
- Date/time captured or uploaded

Decrypted traffic in a DecryptedTraffic table:
- ID (unique)
- Data (points to a file, say /var/dionaea/traffic/<random string>)
- Date/time captured or uploaded
- Source IP
- Destination IP
- Source Port
- Dest Port
- Protocol
- Information about the original SSL traffic
 SSL/TLS version

We might want to store some fields in a free-text XML field because there's little value in making full-fledged table columns when we won't be indexing or searching on those fields. I could go either way.

Each File row would have a one-to-one relationship with an Incident row:
- ID (unique)
- Type {packet capture, decrypted traffic, file}
- Captured or Uploaded
- File or Traffic table ID
- File type
- Flexible XML text, which would include
 the DIS verdict } the DIS verdict is File-specific but it was mentioned that
 the Oracle verdict } changes are being made to DIS to accept captured packets

We'd have an IntrusionAttempt_Incidents table comprised of multiple Incidents:
- IntrusionAttempt ID
- Incident ID

An IntrusionAttempt table:

- IntrusionAttempt ID (unique)
- Flexible XML text
 the analysts' comments
 resolution of the incident -> is it known, a duplicate, or has a new
report been written about it

Perhaps an Intruders table:
- IntrusionAttempt ID
- IP address
- XML
 nmap results
 OS detected

Perhaps a References table:
- IntrusionAttempt ID
- ReferenceType ID
- Reference ID

ReferenceTypes:
- ReferenceType ID (unique)
- Free text ("BID", "MCID", "ARIS Report", "Another IntrusionAttempt"...)

IntrusionAttempts are built by the Honey Pot Monitoring & Management (files and traffic recovered from an intrusion will be combined to form an IntrusionAttempt), or manually by the analyst.
We're assuming that the UI will allow an analyst to manually submit a file acquired through other means (acquired in the wild, or given to us by a partner) to take advantage of the automatic type checking, oracle checking, and DIS uploads.

Elias Levy
2002-12-13 01:11 PM

To: Mario Van Velzen/Calgary/Alberta/SYMANTEC@SYMANTEC
cc: Craig Davison/Calgary/Alberta/SYMANTEC@SYMANTEC
Subject: Re: DeepSight AQS

Regarding the database, how much data to we want to store in it? In an ideal world any information we may learn from the intrusion would be stored in the database. Such things as what foreign IPs where seen, what OS did the fingerprinting tool guess, what attacks did Snort see, what files where modified, removed, or added, etc. But all that means we need to design tables for the information and create tools to parse the output of Snort and other such tools and insert it into the database.

Thoughts?

Elias Levy
Symantec
Alea jacta est

Mario Van Velzen
12/12/2002 02:28 PM

To: Elias Levy/Redwood City/Cal/SYMANTEC@SYMANTEC
cc: Craig Davison/Calgary/Alberta/SYMANTEC@SYMANTEC
Subject: DeepSight AQS

Hi Elias,

At what stage is the AQS FS documentation at? Could you send us the latest
copy?

And apart from the FS, what have you worked on in terms of code and
interface? Let me know.

Cheers,

Mario Van Velzen, mario_vanvelzen@symantec.com
DeepSight Threat Analyst Manager, Symantec

Principal: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
InetSendTo: .
InetCopyTo: elias_levy@symantec.com
InetBlindCopyTo:
$StorageTo: .
$StorageCc: 1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID: <OF6E1C7ACC.DA3AB57E-ON87256C9F.0060142B-87256C9F.0O686EE5@LocalDomain>
INetFrom: craig_davison@symantec.com
PostedDate: 12/30/2002 12:00:41 PM
Recipients: mvelzen@securityfocus.com,CN=Elias Levy/OU=Redwood
City/OU=Cal/O=SYMANTEC@SYMANTEC
$UpdatedBy: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
MailOptions: 0
SaveOptions: 1
From: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
AltFrom: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo: stdNotesLtr0
useApplet: True
Sign: 0
Encrypt:
DefaultMailSaveOptions: 1
Query_String:
SendTo: mvelzen@securityfocus.com
CopyTo: CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
BlindCopyTo:
Subject: The FS section 6.1.5 you asked me to comment on
EnterSendTo: Mario Van Velzen
EnterCopyTo: CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC
EnterBlindCopyTo:

I think Elias has already laid out the best way to do this. He mentions
the specific requirements we have:
We have to capture packets at two places per honeypot (incoming on the
single external interface, and outgoing on the Honeypot interface), and
produce a single file with data captured from both places.

None of the tools based on libpcap (ie, snort, which is very similar to
tcpdump in capture mode) do this for us. They write to a single file, or a
single file per interface if we run multiple instances, but that's not
what we want. We could use libpcap, but not without using multiple threads

or processes, which:
- Is probably more work than just writing the capture code ourselves by opening a kernel Packet Socket
- Does not fit with the model Elias has used in the FS of multiple small utilities running in a single process

We also want to tie this work together with the rest of the project, ie. have it start and stop automatically when we want to start monitoring a Honeypot. Plus, we can still use libpcap to do the "hard" part (formatting the packet output in the tcpdump format, and making sure it conforms to the format).

Still, there is an alternative to Elias' method. If you prefer that we use the tcpdump/snort utilities directly without touching libpcap (except to parse tcpdump logs), we could have one instance per interface (1 external + n Honeypot interfaces) logging to different files, and we could split the output from there by doing some text parsing. I think this method is uglier in that sense, but not necessarily more work. We'd just need to make sure that the copies of tcpdump/snort stayed running (perhaps have a watchdog process).
Basically, the capture would "start" for a Honeypot by looking at two files - the "external" tcpdump log, and the tcpdump log for the Honeypot. Our code would combine:
- all traffic from the Honeypot tcpdump log ("outbound from the Honeypot")
- traffic destined for the Honeypot's IP address, MAC address and broadcast traffic from the external tcpdump log ("inbound to the Honeypot")

As I said, though, I prefer the solution already in the FS.

$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID: <OFC1E08062.923584D8-ON87256CA0.0002783F-87256CA0.00029FF9@LocalDomain>
INetFrom: craig_davison@symantec.com
PostedDate: 12/30/2002 05:28:43 PM
Recipients: mvelzen@securityfocus.com
$UpdatedBy: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
MailOptions: 0
SaveOptions: 1
$Links:
$AltNameLanguageTags:
$StorageCc: 1,.
$StorageTo: 1
$StorageBcc:
InetCopyTo: elias_levy@symantec.com,.
InetSendTo: elias_levy@symantec.com
AltCopyTo:
InetBlindCopyTo:
InheritedReplyTo:
InheritedFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
InheritedAltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
InheritedFromDomain:
From: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
AltFrom: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo: stdNotesLtr0
Sign: 0
Encrypt:
DefaultMailSaveOptions: 1
Query_String:
Principal: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
SendTo: CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
CopyTo: CN=Elias Levy/OU=Redwood

City/OU=Cal/O=SYMANTEC@symantec,mvelzen@securityfocus.com
BlindCopyTo:
Subject: Re: The FS section 6.1.5 you asked me to comment on
$SealData:
EnterSendTo: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
EnterCopyTo: CN=Elias Levy/OU=Redwood
City/OU=Cal/O=SYMANTEC@symantec,mvelzen@securityfocus.com
EnterBlindCopyTo:
$Seal:

Exhibit D

Principal: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
$AutoSpell: 1
$FILE:
AltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo: stdNotesLtr0
useApplet: True
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:
Subject: Draft AQS FS
SendTo: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
CopyTo: CN=Oliver Friedrichs/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC,CN=Alfred Huger/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
InetSendTo: mario_vanvelzen@symantec.com,craig_davison@symantec.com
InetCopyTo: oliver_friedrichs@symantec.com,alfred_huger@symantec.com
$StorageTo: 1,1
$StorageCc: 1,1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
From: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom: elias_levy@symantec.com
$MessageID: <OFBD5A3A28.9B434112-ON88256C9F.00630B14-88256C9F.00634042@LocalDomain>
PostedDate: 12/30/2002 10:57:34 AM
$Signature:
Sign: 0
$Seal:
RoutingState:
$UpdatedBy: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: BD5A3A289B43411288256C9F00630B14
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 12/30/2002 10:57:39 AM-12/30/2002 10:57:39 AM
$MsgTrackFlags: 0
DeliveredDate: 12/30/2002 10:57:39 AM

This is the latest draft. There is little change from the last one since I been working on the mockup web interface. I will be consolidating the event tables into a single one.

Elias Levy
Symantec
Alea jacta est

Exhibit E

```
BEGIN:VCALENDAR
VERSION:2.0
PRODID:-//Apple Inc.//iCal 4.0//EN
CALSCALE:GREGORIAN
BEGIN:VTIMEZONE
TZID:US/Pacific
BEGIN:STANDARD
TZOFFSETFROM:-0700
RRULE:FREQ=YEARLY;UNTIL=20061029T090000Z;BYMONTH=10;BYDAY=-1SU
DTSTART:19621028T020000
TZNAME:PST
TZOFFSETTO:-0800
END:STANDARD
BEGIN:DAYLIGHT
TZOFFSETFROM:-0800
RRULE:FREQ=YEARLY;UNTIL=20060402T100000Z;BYMONTH=4;BYDAY=1SU
DTSTART:19870405T020000
TZNAME:PDT
TZOFFSETTO:-0700
END:DAYLIGHT
BEGIN:DAYLIGHT
TZOFFSETFROM:-0800
RRULE:FREQ=YEARLY;BYMONTH=3;BYDAY=2SU
DTSTART:20070311T020000
TZNAME:PDT
TZOFFSETTO:-0700
END:DAYLIGHT
BEGIN:STANDARD
TZOFFSETFROM:-0700
RRULE:FREQ=YEARLY;BYMONTH=11;BYDAY=1SU
DTSTART:20071104T020000
TZNAME:PST
TZOFFSETTO:-0800
END:STANDARD
END:VTIMEZONE
BEGIN:VEVENT
CREATED:20080324T210223Z
UID:D15987563
DTEND;TZID=US/Pacific:20021231T130000
TRANSP:OPAQUE
SUMMARY:AQS meeting
DTSTART;TZID=US/Pacific:20021231T100000
DTSTAMP:20061227T172209Z
SEQUENCE:0
END:VEVENT
END:VCALENDAR
```

Exhibit F

Received: from uscu-navgw3.symantec.com ([155.64.1.176]) by uscu-smtpib01-1.symantec.com (Lotus Domino Release 5.0.11) with SMTP id 2003010814053070:538370 ; Wed, 8 Jan 2003 14:05:30 -0800
Received: from uscu-navieg.symantec.com ([155.64.1.175]) by uscu-navgw3.symantec.com (SAVSMTP 3.0.0.44ccantisp8) with SMTP id M2003010813574831688 for <Craig_Davison@notes.symantec.com>; Wed, 08 Jan 2003 13:57:48 -0800
Received: from excu-mxib-1.symantec.com ([198.6.49.87]) by uscu-navieg.symantec.com (SAVSMTP 3.0.1.45) with SMTP id M2003010813575021653 for <Craig_Davison@notes.symantec.com>; Wed, 08 Jan 2003 13:57:50 -0800
Received: from securityfocus.com (mail.securityfocus.com [205.206.231.9]) by excu-mxib-1.symantec.com (8.12.2+Sun/8.12.2) with SMTP id h08LvnbI023202 for <Craig_Davison@symantec.com>; Wed, 8 Jan 2003 13:57:50 -0800 (PST)
Received: (qmail 6701 invoked by uid 1016); 8 Jan 2003 21:48:38 -0000
Delivered_To: cd@securityfocus.com
Received: (qmail 6684 invoked by uid 1053); 8 Jan 2003 21:48:37 -0000
PostedDate: 01/08/2003 02:48:37 PM
From: Mario van Velzen <mvelzen@securityfocus.com>
SendTo: Craig Davison <cd@securityfocus.com>,<aleph1@securityfocus.com>
Subject: Re: another developer?
In_Reply_To:
<OF5A62444A.8071D792-ON87256CA8.00772260-87256CA8.007748A4@symantec.com>
$MessageID: <Pine.LNX.4.43.0301081442210.19623-100000@mail.securityfocus.com>
MIME_Version: 1.0
$MIMETrack: Itemize by SMTP Server on USCU-SMTPIB01-1/GLOBE-ADMIN/SYMANTEC(Release 5.0.11 |July 24, 2002) at 01/08/2003 02:05:30 PM,MIME-CD by Notes Client on Craig Davison/Enterprise(Release 6.0.2CF1|June 9, 2003) at 02/27/2009 12:49:18 PM,MIME-CD complete at 02/27/2009 12:49:18 PM
SMTPOriginator: mvelzen@securityfocus.com
RoutingState:
$UpdatedBy: ,CN=USCU-SMTPIB01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteServers:
CN=USCU-SMTPIB01-1/OU=GLOBE-ADMIN/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/08/2003 03:05:30 PM-01/08/2003 03:05:32 PM,01/08/2003 02:51:06 PM-01/08/2003 02:51:06 PM
$Orig: 33ACE5952962212D88256CA800795AAE
Categories:
$Revisions:
$MsgTrackFlags: 0
DeliveredDate: 01/08/2003 02:51:06 PM

Hi there,

That's not quite the whole story. Further along in the project, there might be some additional developers/analysts available for short periods of time.

I have to block off possible sections/parts of the project which could be suitable for people with very short/no ramp-up time. Some of this (especially the analyst teams) has already been written up in the virtual project plan. Other stuff I just became aware of.

In other news:

I'm going to start a MS Project plan for the project, as the AQS is now going to be tracked as a full deliverable, according to all Symantec rules. You should see the start of that on Monday.

We also received some documents regarding the implementation of the malicious code oracle within the DIS system. I will forward that to you.

Also on Monday, would you be available for a meeting on the IRC server, inside the lab?

Let me know if you have any questions.

Thanks,

Mario

> Ben told me on Monday that another developer (spending all or half of their
> time) was being considered for the project. Do either of you have any other
> information about that?

Exhibit G

Received: from uscu-navgw3.symantec.com ([155.64.1.176]) by uscu-smtpib01-2.symantec.com (Lotus Domino Release 5.0.11) with SMTP id 2003011511221509:1039549 ; Wed, 15 Jan 2003 11:22:15 -0800
Received: from uscu-navieg.symantec.com ([155.64.1.175]) by uscu-navgw3.symantec.com (SAVSMTP 3.0.0.44ccantisp8) with SMTP id M2003011511253714811 for <Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003 11:25:37 -0800
Received: from excu-mxib-1.symantec.com ([198.6.49.87]) by uscu-navieg.symantec.com (SAVSMTP 3.0.1.45) with SMTP id M2003011511253908843 for <Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003 11:25:39 -0800
Received: from securityfocus.com (mail.securityfocus.com [205.206.231.9]) by excu-mxib-1.symantec.com (8.12.2+Sun/8.12.2) with SMTP id h0FJPcbI026441 for <Craig_Davison@symantec.com>; Wed, 15 Jan 2003 11:25:39 -0800 (PST)
Received: (qmail 20685 invoked by uid 1016); 15 Jan 2003 19:15:33 -0000
Delivered-To: cd@securityfocus.com
Received: (qmail 20677 invoked by uid 1053); 15 Jan 2003 19:15:32 -0000
PostedDate: 01/15/2003 12:15:32 PM
From: Mario van Velzen <mvelzen@securityfocus.com>
SendTo: Craig Davison <cd@securityfocus.com>,<aleph1@securityfocus.com>
Subject: email for discussion
$MessageID: <Pine.LNX.4.43.0301151054540.1254-100000@mail.securityfocus.com>
MIME_Version: 1.0
$MIMETrack: Itemize by SMTP Server on USCU-SMTPIB01-2/GLOBE-ADMIN/SYMANTEC(Release 5.0.11 |July 24, 2002) at 01/15/2003 11:22:15 AM,MIME-CD by Notes Client on Craig Davison/Enterprise(Release 6.0.2CF1|June 9, 2003) at 02/27/2009 12:49:19 PM,MIME-CD complete at 02/27/2009 12:49:19 PM
SMTPOriginator: mvelzen@securityfocus.com
RoutingState:
$UpdatedBy: ,CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC
RouteServers:
CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/15/2003 12:22:15 PM-01/15/2003 12:22:17 PM,01/15/2003 12:18:51 PM-01/15/2003 12:18:52 PM
$Orig: 0D4B0C47AB3DBAB888256CAF006A6845
Categories:
$Revisions:
$MsgTrackFlags: 0
DeliveredDate: 01/15/2003 12:18:52 PM

Hi there,

PS: There's a few more points I need to touch, but I will send this email out and go from there. Expect more emails from me today and tomorrow. mvv

A few points that we need to touch on. I will write down its current state, and you can let me know if you have any concerns.

- Elias: When would you be available for a meeting? This afternoon or tomorrow? How was your move?

- Craig/Elias: Is Monday appropriate for meetings? Next Monday ok for the both of you?

- Hardware: Here's the current situation:

energon (external: 207.34.103.195, internal: 10.0.2.1)
SSH gateway, running RedHat 8.0, KVM Switch ID 7

fury (internal: 10.0.2.12)
IRC, documents store, CVS

Running RedHat 8.0, KVM Switch ID 1

megatron (internal: 10.0.2.5)
MS SQL
Running W2K Server, KVM Switch ID 3

axe (internal: 10.0.2.6)
Development box
Running RedHat 8.0, KVM Switch ID 2

grimlock (internal: 10.0.2.3)
VMware host
Running RedHat 8.0, KVM Switch ID 5

I will add one box to dedicate it to network processing. Is that appropriate? What else do you need?

- Project plan: The AQS has been promoted to a official Symantec deliverable, which means I have to provide additional information, including a timeline, for the project.

I'm assembling the requirements, and creating a timeline for this. I will send a very rough sketch of it this afternoon, for you to review. Would it be possible for you to review those dates, and modify/buy off on them?

I apologize if those are non-technical issues, but that's what I'm tackled with right now. Let me know if you have any concerns or questions.

Mario

□
$AltNameLanguageTags:
InheritedReplyTo:
InheritedFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
InheritedAltFrom: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
InheritedFromDomain:
AltFrom: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo: StdNotesLtr0
Sign: 0
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:
Principal: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
Subject: Re: Network Space
$SealData:
SendTo: CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
CopyTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
InetSendTo: elias_levy@symantec.com
InetCopyTo: craig_davison@symantec.com
$StorageTo: 1
$StorageCc: 1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
From: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
INetFrom: mario_vanvelzen@symantec.com
$UpdatedBy: CN=Mario Van
Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$MessageID: <OF38FD60B8.8B69BE9B-ON87256CAF.006BCC19-87256CAF.006E018D@LocalDomain>
PostedDate: 01/15/2003 12:51:49 PM
$Seal:
$Orig: 38FD60B88B69BE9B87256CAF006BCC19

```
Categories:
$Revisions:
RouteServers:  CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes:  01/15/2003 12:51:50 PM-01/15/2003 12:51:51 PM
$MsgTrackFlags:  0
DeliveredDate:  01/15/2003 12:51:51 PM

Received:  from uscu-navgw3.symantec.com ([155.64.1.176])          by
uscu-smtpib01-2.symantec.com (Lotus Domino Release 5.0.11)          with SMTP id
2003011511574948:1042566 ;          Wed, 15 Jan 2003 11:57:49 -0800
Received:  from uscu-navieg.symantec.com ([155.64.1.175]) by
uscu-navgw3.symantec.com (SAVSMTP 3.0.0.44ccantisp8) with SMTP id
M2003011512011112501 for <Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003
12:01:11 -0800
Received:  from excu-mxib-1.symantec.com ([198.6.49.87]) by uscu-navieg.symantec.com
(SAVSMTP 3.0.1.45) with SMTP id M2003011512011328654 for
<Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003 12:01:13 -0800
Received:  from securityfocus.com (mail.securityfocus.com [205.206.231.9])      by
excu-mxib-1.symantec.com (8.12.2+Sun/8.12.2) with SMTP id h0FK1DbI005750        for
<Craig_Davison@symantec.com>; Wed, 15 Jan 2003 12:01:13 -0800 (PST)
Received:  (qmail 28305 invoked by uid 1016); 15 Jan 2003 19:51:07 -0000
Delivered_To:  cd@securityfocus.com
Received:  (qmail 28296 invoked by uid 101); 15 Jan 2003 19:51:07 -0000
PostedDate:  01/15/2003 12:51:07 PM
From:  aleph1@securityfocus.com
SendTo:  Mario van Velzen <mvelzen@securityfocus.com>
CopyTo:  Craig Davison <cd@securityfocus.com>
Subject:  Re: email for discussion
$MessageID:  <20030115195107.GB3819@securityfocus.com>
References:  <Pine.LNX.4.43.0301151054540.1254-100000@mail.securityfocus.com>
MIME_Version:  1.0
In_Reply_To:  <Pine.LNX.4.43.0301151054540.1254-100000@mail.securityfocus.com>
$MIMETrack:  Itemize by SMTP Server on USCU-SMTPIB01-2/GLOBE-ADMIN/SYMANTEC(Release
5.0.11  |July 24, 2002) at 01/15/2003 11:57:49 AM,MIME-CD by Notes Client on Craig
Davison/Enterprise(Release 6.0.2CF1|June 9, 2003) at 02/27/2009 12:49:19 PM,MIME-CD
complete at 02/27/2009 12:49:19 PM
SMTPOriginator:  aleph1@securityfocus.com
RoutingState:
$UpdatedBy:  ,CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC
RouteServers:
CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMAN
TEC
RouteTimes:  01/15/2003 12:57:49 PM-01/15/2003 12:57:51 PM,01/15/2003 12:54:25
PM-01/15/2003 12:54:25 PM
$Orig:  AA72BC0C48EB503B88256CAF006DAA04
Categories:
$Revisions:
$MsgTrackFlags:  0
DeliveredDate:  01/15/2003 12:54:25 PM

* Mario van Velzen (mvelzen@securityfocus.com) [030115 19:15]:
> Hi there,
>
> PS: There's a few more points I need to touch, but I will send this email
> out and go from there. Expect more emails from me today and tomorrow. mvv
>
>
> A few points that we need to touch on. I will write down its current
> state, and you can let me know if you have any concerns.
>
> - Elias: When would you be available for a meeting? This afternoon or
> tomorrow? How was your move?
```

Mostly done, but I've found out that the phone wiring inside the house
is crazy. I haven't been able to get a phone line until now. Best call
me on my cell phone. I am available this afternoon if you need me to be
it would be best for me tomorrow.

>
> - Craig/Elias: Is Monday appropriate for meetings? Next Monday ok for the
> both of you?

Yes.

>
> - Hardware: Here's the current situation:
>
> energon (external: 207.34.103.195, internal: 10.0.2.1)
>   SSH gateway, running RedHat 8.0, KVM Switch ID 7
>
> fury (internal: 10.0.2.12)
>   IRC, documents store, CVS
>   Running RedHat 8.0, KVM Switch ID 1
>
> megatron (internal: 10.0.2.5)
>   MS SQL
>   Running W2K Server, KVM Switch ID 3
>
> axe (internal: 10.0.2.6)
>   Development box
>   Running RedHat 8.0, KVM Switch ID 2
>
> grimlock (internal: 10.0.2.3)
>   VMware host
>   Running RedHat 8.0, KVM Switch ID 5
>
> I will add one box to dedicate it to network processing. Is that
> appropriate? What else do you need?

How is axe different from grimlock? We need one box for the actual
VMware service, one box for the honey pot support services (DNS, DHCP),
one box for the NAT system, one box for port scanning, and one box
for malware oracle.
>
> - Project plan: The AQS has been promoted to a official Symantec
> deliverable, which means I have to provide additional information,
> including a timeline, for the project.
>
> I'm assembling the requirements, and creating a timeline for this. I will
> send a very rough sketch of it this afternoon, for you to review. Would
it
> be possible for you to review those dates, and modify/buy off on them?

Tonight, yes.

> I apologize if those are non-technical issues, but that's what I'm
tackled
> with right now. Let me know if you have any concerns or questions.
>
> Mario

--
Elias Levy
Symantec
Alea jacta est

$AutoSpell: 1
$AltNameLanguageTags:
InheritedReplyTo:
InheritedFrom: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedAltFrom: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
InheritedFromDomain:
AltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo: stdNotesLtr0
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:
Principal: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Subject: Re: diagrams sort of wrong
$SealData:
SendTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
CopyTo:
InetSendTo: craig_davison@symantec.com
InetCopyTo:
$StorageTo: 1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
From: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom: elias_levy@symantec.com
$MessageID: <OFD7422AD5.8B04F258-ON88256CAF.006E3B59-88256CAF.006E7299@LocalDomain>
PostedDate: 01/15/2003 12:59:47 PM
$SealData:
Sign: 0
$Seal:
$UpdatedBy: CN=Elias
Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: D7422AD58B04F25888256CAF006E3B59
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/15/2003 12:59:49 PM-01/15/2003 12:59:49 PM
$MsgTrackFlags: 0
DeliveredDate: 01/15/2003 12:59:49 PM

$AutoSpell: 1
$Links:
$AltNameLanguageTags:
InheritedReplyTo:
InheritedFrom: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedAltFrom: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedFromDomain:
AltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo: stdNotesLtr0
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:
Principal: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Subject: Re: Network Space
$SealData:
SendTo: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
CopyTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Elias
Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
InetSendTo: mario_vanvelzen@symantec.com
InetCopyTo: craig_davison@symantec.com,elias_levy@symantec.com
$StorageTo: 1
$StorageCc: 1,1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002

From: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom: elias_levy@symantec.com
$MessageID: <OFEB179A7D.931F96D1-ON88256CAF.006E96D2-88256CAF.006EE870@LocalDomain>
PostedDate: 01/15/2003 01:04:49 PM
$SealData:
Sign: 0
$Seal:
$UpdatedBy: CN=Elias
Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: EB179A7D931F96D188256CAF006E96D2
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/15/2003 01:04:52 PM-01/15/2003 01:04:53 PM
$MsgTrackFlags: 0
DeliveredDate: 01/15/2003 01:04:53 PM

Received: from uscu-navgw3.symantec.com ([155.64.1.176]) by
uscu-smtpib01-2.symantec.com (Lotus Domino Release 5.0.11) with SMTP id
2003011513401000:1049644 ; Wed, 15 Jan 2003 13:40:10 -0800
Received: from uscu-navieg.symantec.com ([155.64.1.175]) by
uscu-navgw3.symantec.com (SAVSMTP 3.0.0.44ccantisp8) with SMTP id
M2003011513433326116 for <Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003
13:43:33 -0800
Received: from excu-mxib-1.symantec.com ([198.6.49.87]) by uscu-navieg.symantec.com
(SAVSMTP 3.0.1.45) with SMTP id M2003011513433421026 for
<Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003 13:43:34 -0800
Received: from securityfocus.com (mail.securityfocus.com [205.206.231.9]) by
excu-mxib-1.symantec.com (8.12.2+Sun/8.12.2) with SMTP id hOFLhXbI027233 for
<Craig_Davison@symantec.com>; Wed, 15 Jan 2003 13:43:34 -0800 (PST)
Received: (qmail 18063 invoked by uid 1016); 15 Jan 2003 21:33:27 -0000
Delivered_To: cd@securityfocus.com
Received: (qmail 18055 invoked by uid 1053); 15 Jan 2003 21:33:27 -0000
PostedDate: 01/15/2003 02:33:27 PM
From: Mario van Velzen <mvelzen@securityfocus.com>
SendTo: aleph1@securityfocus.com
CopyTo: Craig Davison <cd@securityfocus.com>
Subject: Re: email for discussion
In_Reply_To: <20030115195107.GB3819@securityfocus.com>
$MessageID: <Pine.LNX.4.43.0301151429110.1254-100000@mail.securityfocus.com>
MIME_Version: 1.0
$MIMETrack: Itemize by SMTP Server on USCU-SMTPIB01-2/GLOBE-ADMIN/SYMANTEC(Release
5.0.11 |July 24, 2002) at 01/15/2003 01:40:10 PM,MIME-CD by Notes Client on Craig
Davison/Enterprise(Release 6.0.2CF1|June 9, 2003) at 02/27/2009 12:49:19 PM,MIME-CD
complete at 02/27/2009 12:49:19 PM
SMTPOriginator: mvelzen@securityfocus.com
RoutingState:
$UpdatedBy: ,CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC
RouteServers:
CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMAN
TEC
RouteTimes: 01/15/2003 02:40:10 PM-01/15/2003 02:40:11 PM,01/15/2003 02:36:45
PM-01/15/2003 02:36:46 PM
$Orig: 2D56674769D61F4188256CAF007708AA
Categories:
$Revisions:
$MsgTrackFlags: 0
DeliveredDate: 01/15/2003 02:36:46 PM

Greetings,

> > - Elias: When would you be available for a meeting? This afternoon or

> > tomorrow? How was your move?
>
> Mostly done, but I've found out that the phone wiring inside the house
> is crazy. I haven't been able to get a phone line until now. Best call
> me on my cell phone. I am available this afternoon if you need me to be
> it would be best for me tomorrow.

Tomorrow is good. 2pm MST = 1pm PST appropriate for everyone?

> > - Craig/Elias: Is Monday appropriate for meetings? Next Monday ok for
the
> > both of you?
>
> Yes.

Again, 2pm MST?

Thanks,

Mario

Received: from uscu-navgw3.symantec.com ([155.64.1.176]) by
uscu-smtpib01-2.symantec.com (Lotus Domino Release 5.0.11) with SMTP id
2003011514232846:1052662 ; Wed, 15 Jan 2003 14:23:28 -0800
Received: from uscu-navieg.symantec.com ([155.64.1.175]) by
uscu-navgw3.symantec.com (SAVSMTP 3.0.0.44ccantisp8) with SMTP id
M2003011514265125255 for <Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003
14:26:51 -0800
Received: from excu-mxib-1.symantec.com ([198.6.49.87]) by uscu-navieg.symantec.com
(SAVSMTP 3.0.1.45) with SMTP id M2003011514265228277 for
<Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003 14:26:52 -0800
Received: from securityfocus.com (mail.securityfocus.com [205.206.231.9]) by
excu-mxib-1.symantec.com (8.12.2+Sun/8.12.2) with SMTP id hOFMQqbIOO6330 for
<Craig_Davison@symantec.com>; Wed, 15 Jan 2003 14:26:52 -0800 (PST)
Received: (qmail 30348 invoked by uid 1016); 15 Jan 2003 22:16:45 -0000
Delivered_To: cd@securityfocus.com
Received: (qmail 30335 invoked from network); 15 Jan 2003 22:16:45 -0000
Received: from navgwout.symantec.com (198.6.49.12) by mail.securityfocus.com with
SMTP; 15 Jan 2003 22:16:45 -0000
Received: from navgwout.symantec.com (navgwout [198.6.49.12]) by
navgwout.symantec.com (8.9.3+Sun/8.9.3) with SMTP id OAA10328; Wed, 15 Jan 2003
14:26:50 -0800 (PST)
Received: from mailer.symantec.com ([198.6.49.176]) by navgwout.symantec.com
(SAVSMTP 3.0.1.45) with SMTP id M2003011514269290 28 ; Wed, 15 Jan 2003 14:26:49
-0800
Received: from uscu-smtpob01-1.symantec.com (uscu-smtpob01-1.symantec.com
[155.64.74.130]) by mailer.symantec.com (8.11.6+Sun/8.11.6) with ESMTP id
hOFMQnB10884; Wed, 15 Jan 2003 14:26:49 -0800 (PST)
Subject: Re: email for discussion
SendTo: Mario van Velzen <mvelzen@securityfocus.com>
CopyTo: aleph1@securityfocus.com,Craig Davison <cd@securityfocus.com>
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID:
<OF5B1OD4B1.827CA148-ON87256CAF.OO7B8AEA-87256CAF.OO7B8FFE@symantec.com>
From: "Craig Davison" <craig_davison@symantec.com>
PostedDate: 01/15/2003 03:29:37 PM
MIME_Version: 1.0
$MIMETrack: Serialize by Router on USCU-SMTPOB01-1/GLOBE-ADMIN/SYMANTEC(Release
5.0.11 |July 24, 2002) at 01/15/2003 02:35:24 PM,Itemize by SMTP Server on
USCU-SMTPIB01-2/GLOBE-ADMIN/SYMANTEC(Release 5.0.11 |July 24, 2002) at 01/15/2003
02:23:28 PM,MIME-CD by Notes Client on Craig Davison/Enterprise(Release

6.0.2CF1|June 9, 2003) at 02/27/2009 12:49:19 PM,MIME-CD complete at 02/27/2009
12:49:19 PM
SMTPOriginator: craig_davison@symantec.com
RoutingState:
$UpdatedBy: ,CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC
RouteServers:
CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMAN
TEC
RouteTimes: 01/15/2003 03:23:28 PM-01/15/2003 03:23:29 PM,01/15/2003 03:20:03
PM-01/15/2003 03:20:04 PM
$Orig: 0E5F1ED776C0224D88256CAF007AFFAE
Categories:
$Revisions:
$MsgTrackFlags: 0
DeliveredDate: 01/15/2003 03:20:04 PM

Yep.

|---------+---------------------------->
	Mario van Velzen
	<mvelzen@security
	focus.com>
	2003-01-15 02:33
	PM
---------+---------------------------->
>--
----------------------------------|
| |
| To:
aleph1@securityfocus.com
|
| cc: Craig Davison
<cd@securityfocus.com>
|
| Subject: Re: email for
discussion
|
>--
----------------------------------|

Greetings,

> > - Elias: When would you be available for a meeting? This afternoon or
> > tomorrow? How was your move?
>
> Mostly done, but I've found out that the phone wiring inside the house
> is crazy. I haven't been able to get a phone line until now. Best call
> me on my cell phone. I am available this afternoon if you need me to be
> it would be best for me tomorrow.

Tomorrow is good. 2pm MST = 1pm PST appropriate for everyone?

> > - Craig/Elias: Is Monday appropriate for meetings? Next Monday ok for
the
> > both of you?

>
> Yes.

Again, 2pm MST?

Thanks,

Mario

Received: from uscu-navgw3.symantec.com ([155.64.1.176]) by uscu-smtpib01-2.symantec.com (Lotus Domino Release 5.0.11) with SMTP id 2003011520302439:1071989 ; Wed, 15 Jan 2003 20:30:24 -0800
Received: from uscu-navieg.symantec.com ([155.64.1.175]) by uscu-navgw3.symantec.com (SAVSMTP 3.0.0.44ccantisp8) with SMTP id M2003011520334503645 for <Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003 20:33:45 -0800
Received: from excu-mxib-1.symantec.com ([198.6.49.87]) by uscu-navieg.symantec.com (SAVSMTP 3.0.1.45) with SMTP id M2003011520334806884 for <Craig_Davison@notes.symantec.com>; Wed, 15 Jan 2003 20:33:48 -0800
Received: from securityfocus.com (mail.securityfocus.com [205.206.231.9]) by excu-mxib-1.symantec.com (8.12.2+Sun/8.12.2) with SMTP id h0G4xmbI007023 for <Craig_Davison@symantec.com>; Wed, 15 Jan 2003 20:33:48 -0800 (PST)
Received: (qmail 10204 invoked by uid 1016); 16 Jan 2003 04:23:39 -0000
Delivered_To: cd@securityfocus.com
Received: (qmail 10196 invoked by uid 101); 16 Jan 2003 04:23:39 -0000
PostedDate: 01/15/2003 09:23:39 PM
From: aleph1@securityfocus.com
SendTo: Mario van Velzen <mvelzen@securityfocus.com>
CopyTo: Craig Davison <cd@securityfocus.com>
Subject: Re: email for discussion
$MessageID: <20030116042339.GB9221@securityfocus.com>
References: <20030115195107.GB3819@securityfocus.com>
<Pine.LNX.4.43.0301151429110.1254-100000@mail.securityfocus.com>
MIME_Version: 1.0
In_Reply_To: <Pine.LNX.4.43.0301151429110.1254-100000@mail.securityfocus.com>
$MIMETrack: Itemize by SMTP Server on USCU-SMTPIB01-2/GLOBE-ADMIN/SYMANTEC(Release 5.0.11 |July 24, 2002) at 01/15/2003 08:30:24 PM,MIME-CD by Notes Client on Craig Davison/Enterprise(Release 6.0.2CF1|June 9, 2003) at 02/27/2009 12:49:19 PM,MIME-CD complete at 02/27/2009 12:49:19 PM
SMTPOriginator: aleph1@securityfocus.com
RoutingState:
$UpdatedBy: ,CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC
RouteServers:
CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/15/2003 09:30:24 PM-01/15/2003 09:30:25 PM,01/15/2003 09:26:58 PM-01/15/2003 09:26:59 PM
$Orig: DDEA728D686296C388256CB00018C1A8
Categories:
$Revisions:
$MsgTrackFlags: 0
DeliveredDate: 01/15/2003 09:26:59 PM

* Mario van Velzen (mvelzen@securityfocus.com) [030115 21:33]:
> Greetings,
>

> > > - Elias: When would you be available for a meeting? This afternoon or
> > > tomorrow? How was your move?
> > >
> > Mostly done, but I've found out that the phone wiring inside the house
> > is crazy. I haven't been able to get a phone line until now. Best call
> > me on my cell phone. I am available this afternoon if you need me to be
> > it would be best for me tomorrow.
>
> Tomorrow is good. 2pm MST = 1pm PST appropriate for everyone?
>
> > > - Craig/Elias: Is Monday appropriate for meetings? Next Monday ok
for the
> > > both of you?
> > >
> > Yes.
>
> Again, 2pm MST?

Yes.

>
> Thanks,
>
> Mario

--
Elias Levy
Symantec
Alea jacta est

Principal: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
$FILE:
AltFrom: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo: StdNotesLtr0
useApplet: True
Sign: 0
DefaultMailSaveOptions: 1
Query_String:
Subject: task list for project plan
SendTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Elias
Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
CopyTo:
InetSendTo: craig_davison@symantec.com,elias_levy@symantec.com
InetCopyTo:
$StorageTo: 1,1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID: <OF4B9CA53F.1B08CD6A-ON87256CB0.0073719D-87256CB0.00738E42@LocalDomain>
From: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
INetFrom: mario_vanvelzen@symantec.com
PostedDate: 01/16/2003 02:02:10 PM
Encrypt:
RoutingState:
$UpdatedBy: CN=Mario Van
Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: 4B9CA53F1B08CD6A87256CB00073719D
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/16/2003 01:52:32 PM-01/16/2003 01:52:33 PM
$MsgTrackFlags: 0

DeliveredDate: 01/16/2003 01:52:33 PM

Hi there,

Attached you will find an outline project plan, with a number of dates
associated with them. We will discuss this at the meeting.

Thanks!

Mario

Principal: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
$AutoSpell: 1
AltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo: stdNotesLtr0
useApplet: True
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:
Subject: Training dates
$SealData:
$SealData:
SendTo: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Craig
Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
CopyTo:
InetSendTo: mario_vanvelzen@symantec.com,craig_davison@symantec.com
InetCopyTo:
$StorageTo: 1,1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
From: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom: elias_levy@symantec.com
$MessageID: <OF6292EF66.C075D624-ON88256CB1.0005207A-88256CB1.000552C8@LocalDomain>
PostedDate: 01/16/2003 05:51:33 PM
$SealData:
Sign: 0
$Seal:
$UpdatedBy: CN=Elias
Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: 6292EF66C075D62488256CB10005207A
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/16/2003 05:51:33 PM-01/16/2003 05:51:33 PM
$MsgTrackFlags: 0
DeliveredDate: 01/16/2003 05:51:33 PM

Principal: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
$AutoSpell: 1
AltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo: stdNotesLtr0
useApplet: True
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:

```
Subject:  Malware Oracle
$SealData:
$SealData:
SendTo:  CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Craig
Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
CopyTo:
InetSendTo:  mario_vanvelzen@symantec.com,craig_davison@symantec.com
InetCopyTo:
$StorageTo:  1,1
$Mailer:  Lotus Notes Release 5.0.9a  January 7, 2002
From:  CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom:  elias_levy@symantec.com
$MessageID:  <OF85BF85F5.5888B940A-ON88256CB1.00006A7CD-88256CB1.00071AC1@LocalDomain>
PostedDate:  01/16/2003 06:11:00 PM
$SealData:
Sign:  0
$Seal:
$UpdatedBy:  CN=Elias
Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig:  85BF85F5588B940A88256CB10006A7CD
Categories:
$Revisions:
RouteServers:  CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes:  01/16/2003 06:11:00 PM-01/16/2003 06:11:00 PM
$MsgTrackFlags:  0
DeliveredDate:  01/16/2003 06:11:00 PM

$FILE:
$AutoSpell:  1
$AltNameLanguageTags:
InheritedReplyTo:
InheritedFrom:  CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedAltFrom:  CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
InheritedFromDomain:
AltFrom:  CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo:  stdNotesLtr0
Encrypt:  1
DefaultMailSaveOptions:  1
Query_String:
Principal:  CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Subject:  Re: task list for project plan
SendTo:  CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
CopyTo:  CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Elias
Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
InetSendTo:  mario_vanvelzen@symantec.com
InetCopyTo:  craig_davison@symantec.com,elias_levy@symantec.com
$StorageTo:  1
$StorageCc:  1,1
$Mailer:  Lotus Notes Release 5.0.9a  January 7, 2002
From:  CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom:  elias_levy@symantec.com
$MessageID:  <OFF2C406DC.B4845282-ON88256CB1.0009A401-88256CB1.0009FCC4@LocalDomain>
PostedDate:  01/16/2003 06:42:25 PM
$Signature:
Sign:  0
$Seal:
RoutingState:
$UpdatedBy:  CN=Elias
Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig:  F2C406DCB484528288256CB10009A401
Categories:
$Revisions:
```

RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/16/2003 06:42:34 PM-01/16/2003 06:42:36 PM
$MsgTrackFlags: 0
DeliveredDate: 01/16/2003 06:42:36 PM

Please switch the Inquisitor FSD with the Malware Oracle one. Remove the SND/DIS FSD, and replace the date for the Malware Oracle FSD with the 2/21 date. I hope it won't take that long but at this time the Malware Oracle is a wild card. Until I learn more from Symantec we better use this latter date.

Elias Levy
Symantec
Alea jacta est

Mario Van Velzen
01/16/2003 01:02 PM

To: Craig Davison/Calgary/Alberta/SYMANTEC@SYMANTEC, Elias Levy/Redwood City/Cal/SYMANTEC@SYMANTEC
cc:
Subject: task list for project plan

Hi there,

Attached you will find an outline project plan, with a number of dates associated with them. We will discuss this at the meeting.

Thanks!

Mario

$AutoSpell: 1
$AltNameLanguageTags:
InheritedReplyTo:
InheritedFrom: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedAltFrom: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
InheritedFromDomain:
AltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo: stdNotesLtr0
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:
Principal: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Subject: Re: HoneyPotAddresses
$SealData:
SendTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
CopyTo: CN=Elias Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
InetSendTo: craig_davison@symantec.com
InetCopyTo: elias_levy@symantec.com
$StorageTo: 1
$StorageCc: 1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
From: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom: elias_levy@symantec.com

$MessageID: <OF458324BF.C348FF01-ON88256CB1.0066F4F3-88256CB1.0067279D@LocalDomain>
PostedDate: 01/17/2003 11:40:07 AM
$SealData:
Sign: 0
$Seal:
$UpdatedBy: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: 458324BFC348FF0188256CB10066F4F3
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/17/2003 11:40:14 AM-01/17/2003 11:40:15 AM
$MsgTrackFlags: 0
DeliveredDate: 01/17/2003 11:40:15 AM

Principal: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
$AutoSpell: 1
AltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo: stdNotesLtr0
useApplet: True
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:
Subject: AQS/DIS Integration
$SealData:
$SealData:
SendTo: CN=Jim Hill/OU=Beaverton/OU=Oregon/O=SYMANTEC@SYMANTEC
CopyTo:
InetSendTo: jhill@symantec.com
InetCopyTo:
$StorageTo: 0
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
From: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom: elias_levy@symantec.com
$MessageID: <OFAA9425CC.2C017B58-ON88256CB1.007055B5-88256CB1.00719C08@LocalDomain>
PostedDate: 01/17/2003 01:34:19 PM
$SealData:
Sign: 0
$Seal:
$UpdatedBy: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: AA9425CC2C017B5888256CB1007055B5
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/17/2003 01:34:26 PM-01/17/2003 01:34:27 PM
$MsgTrackFlags: 0
DeliveredDate: 01/17/2003 01:34:27 PM
BlindCopyTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
InetBlindCopyTo: craig_davison@symantec.com
$StorageBcc: 1

Principal: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
AltFrom: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo: StdNotesLtr0
useApplet: True
Sign: 0

DefaultMailSaveOptions: 1
Query_String:
Subject: comments on timeline?
SendTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,cd@securityfocus.com
CopyTo:
InetSendTo: craig_davison@symantec.com,.
InetCopyTo:
$StorageTo: 1,.
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID: <OF8DD57233.6C442621-ON87256CB3.007E1244-87256CB3.007E263A@LocalDomain>
From: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
INetFrom: mario_vanvelzen@symantec.com
PostedDate: 01/19/2003 03:57:53 PM
Encrypt:
$UpdatedBy: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
$Orig: 8DD572336C44262187256CB3007E1244
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/19/2003 03:47:57 PM-01/19/2003 03:47:58 PM
$MsgTrackFlags: 0
DeliveredDate: 01/19/2003 03:47:58 PM

Hi there,

I still have not received your comments/edits on the timeline. Can you send them to me first thing Monday morning?

Thanks,

Mario

Received: from uscu-navgw3.symantec.com ([155.64.1.176]) by uscu-smtpib01-2.symantec.com (Lotus Domino Release 5.0.11) with SMTP id 2003011914551181:1171783 ; Sun, 19 Jan 2003 14:55:11 -0800
Received: from uscu-navieg.symantec.com ([155.64.1.175]) by uscu-navgw3.symantec.com (SAVSMTP 3.0.0.44ccantisp8) with SMTP id M2003011914583512568 for <Craig_Davison@notes.symantec.com>; Sun, 19 Jan 2003 14:58:35 -0800
Received: from excu-mxib-1.symantec.com ([198.6.49.87]) by uscu-navieg.symantec.com (SAVSMTP 3.0.1.45) with SMTP id M2003011914583716371 for <Craig_Davison@notes.symantec.com>; Sun, 19 Jan 2003 14:58:37 -0800
Received: from securityfocus.com (mail.securityfocus.com [205.206.231.9]) by excu-mxib-1.symantec.com (8.12.2+Sun/8.12.2) with SMTP id hOJMwZbIO12477 for <Craig_Davison@symantec.com>; Sun, 19 Jan 2003 14:58:35 -0800 (PST)
Received: (qmail 18752 invoked by uid 1016); 19 Jan 2003 22:47:57 -0000
Delivered_To: cd@securityfocus.com
Received: (qmail 30251 invoked from network); 19 Jan 2003 22:44:17 -0000
Received: from navgwout.symantec.com (198.6.49.12) by mail.securityfocus.com with SMTP; 19 Jan 2003 22:44:17 -0000
Received: from navgwout.symantec.com (navgwout [198.6.49.12]) by navgwout.symantec.com (8.9.3+Sun/8.9.3) with SMTP id OAA00293 for <cd@securityfocus.com>; Sun, 19 Jan 2003 14:54:53 -0800 (PST)
Received: from mailer.symantec.com ([198.6.49.176]) by navgwout.symantec.com (SAVSMTP 3.0.1.45) with SMTP id M2003011914545224590 for <cd@securityfocus.com>; Sun, 19 Jan 2003 14:54:52 -0800
Received: from uscu-smtpob01-1.symantec.com (uscu-smtpob01-1.symantec.com [155.64.74.130]) by mailer.symantec.com (8.11.6+Sun/8.11.6) with ESMTP id hOJMsqB20427 for <cd@securityfocus.com>; Sun, 19 Jan 2003 14:54:52 -0800 (PST)
Subject: comments on timeline?

SendTo: "Craig Davison" <craig_davison@symantec.com>,cd@securityfocus.com
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID:
<OF8DD57233.6C442621-ON87256CB3.007E1244-87256CB3.007E263A@symantec.com>
From: "Mario Van Velzen" <mario_vanvelzen@symantec.com>
PostedDate: 01/19/2003 03:57:53 PM
MIME_Version: 1.0
$MIMETrack: Serialize by Router on USCU-SMTPOB01-1/GLOBE-ADMIN/SYMANTEC(Release
5.0.11 |July 24, 2002) at 01/19/2003 03:03:31 PM,Itemize by SMTP Server on
USCU-SMTPIB01-2/GLOBE-ADMIN/SYMANTEC(Release 5.0.11 |July 24, 2002) at 01/19/2003
02:55:11 PM,MIME-CD by Notes Client on Craig Davison/Enterprise(Release
6.0.2CF1|June 9, 2003) at 02/27/2009 12:49:19 PM,MIME-CD complete at 02/27/2009
12:49:19 PM
SMTPOriginator: mario_vanvelzen@symantec.com
RoutingState:
$UpdatedBy: ,CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC
RouteServers:
CN=USCU-SMTPIB01-2/OU=GLOBE-ADMIN/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMAN
TEC
RouteTimes: 01/19/2003 03:55:11 PM-01/19/2003 03:55:13 PM,01/19/2003 03:51:45
PM-01/19/2003 03:51:45 PM
$Orig: C90952B70421B57888256CB3007DE72F
Categories:
$Revisions:
$MsgTrackFlags: 0
DeliveredDate: 01/19/2003 03:51:45 PM

Hi there,

I still have not received your comments/edits on the timeline. Can you send
them to me first thing Monday morning?

Thanks,

Mario

$FILE:
$Links:
$AltNameLanguageTags:
InheritedReplyTo:
InheritedFrom: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedAltFrom: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedFromDomain:
AltFrom: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
Logo: StdNotesLtr0
Sign: 0
DefaultMailSaveOptions: 1
Query_String:
Principal: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
Subject: Re: task list for project plan
SendTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Elias
Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
CopyTo:
InetSendTo: craig_davison@symantec.com,elias_levy@symantec.com
InetCopyTo:
$StorageTo: 1,1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
$MessageID: <OF808E0AD3.B9A0D1F2-ON87256CB4.00677E82-87256CB4.0067A249@LocalDomain>
From: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
INetFrom: mario_vanvelzen@symantec.com
PostedDate: 01/20/2003 11:51:57 AM

Encrypt:
RoutingState:
$UpdatedBy: CN=Mario Van
Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: 808E0AD3B9A0D1F287256CB400677E82
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/20/2003 11:42:33 AM-01/20/2003 11:42:34 AM
$MsgTrackFlags: 0
DeliveredDate: 01/20/2003 11:42:34 AM

Hi there,

Here is the updated calendar, with both your changes, and holidays added
for both Canada and US sites. Are you all in agreement with the dates?

Let me know either way. Thank you.

Mario

Craig Davison
01/20/2003 10:35 AM

To: Mario Van Velzen/Calgary/Alberta/SYMANTEC@SYMANTEC
cc: Elias Levy/Redwood City/Cal/SYMANTEC@symantec
Subject: Re: task list for project plan

All the dates look fine to me except for:
- Management Console/UI. Although the UI is simple in this project, UI
development is time-consuming and plenty of small things can go wrong.
15 days?
- Inquisitor. This is a simple component, true, but I don't think 5 days
is a safe estimate for any one piece of the project.
8 days?

Mario Van Velzen
2003-01-16 02:02 PM

To: Craig Davison/Calgary/Alberta/SYMANTEC@SYMANTEC, Elias
Levy/Redwood
City/Cal/SYMANTEC@SYMANTEC
cc:
Subject: task list for project plan

Hi there,

Attached you will find an outline project plan, with a number of dates
associated with them. We will discuss this at the meeting.

Thanks!

Mario

$FILE:
$AutoSpell: 1
$Links:
$AltNameLanguageTags:
InheritedReplyTo:
InheritedFrom: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedAltFrom: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC
InheritedFromDomain:
AltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo: stdNotesLtr0
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:
Principal: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Subject: Re: task list for project plan
SendTo: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
CopyTo: CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Elias
Levy/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
InetSendTo: mario_vanvelzen@symantec.com
InetCopyTo: craig_davison@symantec.com,elias_levy@symantec.com
$StorageTo: 1
$StorageCc: 1,1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
From: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom: elias_levy@symantec.com
$MessageID: <OF4D20F148.9B99A12B-ON88256CB4.00775F45-88256CB4.00778B13@LocalDomain>
PostedDate: 01/20/2003 02:39:01 PM
$Signature:
Sign: 0
$Seal:
RoutingState:
$UpdatedBy: CN=Elias
Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: 4D20F1489B99A12B88256CB400775F45
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/20/2003 02:39:16 PM-01/20/2003 02:39:16 PM
$MsgTrackFlags: 0
DeliveredDate: 01/20/2003 02:39:16 PM

In general it looks good. The only caveat is the time set aside for the
malware oracle FSD. We need more information from Symantec. But for now is
as good an estimate as any.

Elias Levy
Symantec
Alea jacta est

Mario Van Velzen
01/20/2003 10:51 AM

To: Craig Davison/Calgary/Alberta/SYMANTEC@SYMANTEC, Elias
Levy/Redwood
City/Cal/SYMANTEC@SYMANTEC
cc:
Subject: Re: task list for project plan

Hi there,

Here is the updated calendar, with both your changes, and holidays added for both Canada and US sites. Are you all in agreement with the dates?

Let me know either way. Thank you.

Mario

Exhibit H

Principal: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
$langprincipal:
$altprincipal: CN=Ben Baker/OU=Eugene/OU=Oregon/O=SYMANTEC
$AutoSpell: 1
$FILE:
AltFrom: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
Logo: stdNotesLtr0
useApplet: True
Encrypt: 1
DefaultMailSaveOptions: 1
Query_String:
Subject: AQS FSD v1.0
SendTo: CN=Mario Van Velzen/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC,CN=Craig Davison/OU=Calgary/OU=Alberta/O=SYMANTEC@SYMANTEC
CopyTo: CN=Oliver Friedrichs/OU=Redwood City/OU=Cal/O=SYMANTEC@SYMANTEC
InetSendTo: mario_vanvelzen@symantec.com,craig_davison@symantec.com
InetCopyTo: oliver_friedrichs@symantec.com
$StorageTo: 1,1
$StorageCc: 1
$Mailer: Lotus Notes Release 5.0.9a January 7, 2002
From: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC
INetFrom: elias_levy@symantec.com
$MessageID: <OF6C65D981.4D3BF8ED-ON88256CB4.002554E6-88256CB4.005FB02C@LocalDomain>
PostedDate: 01/20/2003 10:18:26 AM
$Signature:
Sign: 0
$Seal:
RoutingState:
$UpdatedBy: CN=Elias Levy/OU=Redwood/OU=Cal/O=SYMANTEC,CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
$Orig: 6C65D9814D3BF8ED88256CB4002554E6
Categories:
$Revisions:
RouteServers: CN=USCU-MAIL01-1/OU=GLOBE-ADMIN/O=SYMANTEC
RouteTimes: 01/20/2003 10:25:18 AM-01/20/2003 10:25:19 AM
$MsgTrackFlags: 0
DeliveredDate: 01/20/2003 10:25:19 AM

Attached is the AQS FSD v1.0.

Elias Levy
Symantec
Alea jacta est

Exhibit I

```
BEGIN:VCALENDAR
VERSION:2.0
PRODID:-//Apple Inc.//iCal 4.0//EN
CALSCALE:GREGORIAN
BEGIN:VTIMEZONE
TZID:US/Pacific
BEGIN:STANDARD
TZOFFSETFROM:-0700
RRULE:FREQ=YEARLY;UNTIL=20061029T090000Z;BYMONTH=10;BYDAY=-1SU
DTSTART:19621028T020000
TZNAME:PST
TZOFFSETTO:-0800
END:STANDARD
BEGIN:DAYLIGHT
TZOFFSETFROM:-0800
RRULE:FREQ=YEARLY;UNTIL=20060402T100000Z;BYMONTH=4;BYDAY=1SU
DTSTART:19870405T020000
TZNAME:PDT
TZOFFSETTO:-0700
END:DAYLIGHT
BEGIN:DAYLIGHT
TZOFFSETFROM:-0800
RRULE:FREQ=YEARLY;BYMONTH=3;BYDAY=2SU
DTSTART:20070311T020000
TZNAME:PDT
TZOFFSETTO:-0700
END:DAYLIGHT
BEGIN:STANDARD
TZOFFSETFROM:-0700
RRULE:FREQ=YEARLY;BYMONTH=11;BYDAY=1SU
DTSTART:20071104T020000
TZNAME:PST
TZOFFSETTO:-0800
END:STANDARD
END:VTIMEZONE
BEGIN:VEVENT
CREATED:20080324T210223Z
UID:D15987639
DTEND;TZID=US/Pacific:20030219T140000
RRULE:FREQ=WEEKLY;INTERVAL=1;UNTIL=20030418T065959Z;BYDAY=WE
TRANSP:OPAQUE
SUMMARY:AQS meeting
DTSTART;TZID=US/Pacific:20030219T130000
DTSTAMP:20061227T172209Z
SEQUENCE:0
END:VEVENT
END:VCALENDAR
```